UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,560	02/09/2004	Young-Hyun Kim	678-1163 (P10820)	1111

28249 7590 02/26/2007

DILWORTH & BARRESE, LLP
333 EARLE OVINGTON BLVD.
SUITE 702
UNIONDALE, NY 11553

EXAMINER	
AHUJA, SUPRIYA	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/774,560	KIM, YOUNG-HYUN	
	Examiner	Art Unit	
	Supriya Ahuja	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/09/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02/09/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities:

On page 2, line 15, the phrase "It is, therefore, an" should be replaced by --The--.

On page 6, line 27, the content server 22 is missing in Fig. 2.

Appropriate correction is required.

Claim Objections

2. **Claims 7-12** are objected to because of the following informalities:

In claim 7, line 2, the phrase "for previously uploaded" should be replaced by --for the previously uploaded--.

In independent claim 8, line 9, the phrase "encrypting content" should be replaced by --encrypting the content--. Dependent claims 9-12 are objected for the same.

In claim 10, line 7, the phrase "if encrypted content" should be replaced by --if the encrypted content--.

In claim 12, line 2, the phrase "when time information" should be replaced by --when the information--.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claim 1** is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al.(US 5,054,064 dated 10/01/1991) in view of Iguchi et al. (US 2002/0169960 dated 11/14/2002).

Walker et al. discloses a video system that includes a central facility (external device) and a terminal. The video system is provided with the video program, which is transmitted, by broadcast, cable, satellite, fiber or any other transmission medium (from the server; col. 2 lines 30 – 32). The terminal includes means for retrieving video programs and sending the program identification data to the central facility. The central facility includes a database for storing and retrieving at least one code encryption code corresponding to the program identification data and means for sending the code encryption key from the central facility to the terminal (abstract). The terminal includes means to store terminal identification data, means to send the central facility the terminal identification data and the program identification data over link (a link is a continuous data channel between a terminal and a central facility such as an ISDN D-channel or by modem a regular phone line (col. 3 lines 46-49)) (col. 2 lines 44-47). The terminal receives the code encryption key from the central facility and decrypts the encrypted digital code (claim 1, lines 14-22). The terminal includes a controller, an encryptor, and a decryptor and recording medium (storage) to store the signal, a memory to store the key and terminal ID (Fig. 1, col. 2 lines 21-45; col. 3 lines 5-15). Terminal includes means to encrypt the terminal identification data according to the terminal specific encryption key, means to send unencrypted terminal identification data and encrypted terminal identification data to the central facility, which in turn includes means to compare unencrypted and encrypted terminal

identification data to verify terminal identity (col 3. lines 15-21). The system preferably uses at least one downloadable key, encrypted video program that uses the key for decryption, and data stored a field of the video program. It may be implemented in all digital, analog or mixed analog/digital environments (col. 4 lines 22-26). DES decryption keys are transmitted from the central facility to the terminal. The DES session key is generated by the central facility at the beginning of the session and remains valid for the duration of the session. The terminal begins the session using a terminal-unique DES key stored in a ROM (col. 5 lines 32-39).

Iguchi et al. discloses a storage device consisting of a tamper-resistant module and a flash memory. Content is downloaded from the server through a mobile terminal [0088]. The mobile terminal consists of a CPU, a RAM, a ROM, a controlling circuit, an I/O interface and a decoder circuit ([0058], Fig. 3). The controller includes an interface for connecting between devices (claim 15). A host interface is used for transmitting/receiving an access command between the storage device and an external appliance connected to the storage device. The input/output interface performs processings such as a key inputting by the user of the mobile terminal and a screen displaying [0041]. The transmission/reception of the information between the storage device and the mobile terminal is performed by the access command. A physical access command is a basic command on an input/output of data or the like with the storage device. A logical access command is transmitted/received as the data for the physical access command [0062-0063].

Walker et al. discloses all the limitations of claim 1 except for a communication unit for providing an interface for exchanging data with the external device and transmitting a download request signal (yourdictionary.com states: download means to transfer (data or programs) from a

server or host computer to one's own computer or device. Similarly upload means to transfer (data or programs), usually from a peripheral computer or device to a central, often remote computer. Therefore, here transmitting or receiving content means downloading or uploading content, as content is being transferred over a network). The general concept of using an interface for communicating information between devices using a request signal is well known in the art as illustrated by Iguchi et al. which discloses a host interface is used for transmitting/receiving an access command between the storage device and an external appliance connected to the storage device [0041]. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al. to include the use of an interface to transmit or receive request signals as taught by Iguchi et al. in order to establish connection with the external devices as stated by Iguchi et al. ([0060], lines 11-13).

5. **Claim 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al.(US 5,054,064 dated 10/01/1991) and Iguchi et al. (US 2002/0169960 dated 11/14/2002) as applied to claim 1 above, and further in view of Choi et al. (US 2002/0194492 dated 12/19/2002).

Walker et al. and Iguchi et al. disclose all the limitations of claim 2 except that the external device generates an encryption key based on the model information and the serial number of the mobile terminal. The general concept of generating an encryption key based on the model information and serial number is well known in the art as illustrated by Choi et al. which discloses a program that generates a system unique encryption key from the unique hardware information (serial number, model information, etc.) of a personal computer [0076]. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al. and Iguchi et al. to include the use of an encryption key generated based on model

information and serial number as taught by Choi et al. in order to limit the access of the content only by a key manager as stated by Choi et al. ([0077] lines 8-11).

6. **Claim 3** is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al.(US 5,054,064 dated 10/01/1991), Iguchi et al. (US 2002/0169960 dated 11/14/2002) and Choi et al. (US 2002/0194492 dated 12/19/2002) as applied to claim 2 above, and further in view of Lennon et al. (US 4193131 dated 03/11/1980).

Walker et al., Iguchi et al. and Choi et al. disclose all the limitations of claim 3 except that the encryption key is generated by the external device considering further time information set in the external device. The general concept of generating encryption keys using time information set is well known in the art as an obvious encryption technique as illustrated by Lennon et al. which discloses a system generated time variant, dynamically created key being transmitted in enciphered form under key encrypting key from a host system to a remote terminal [col. 6 lines 27-31]. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al., Iguchi et al, and Choi et al. to include the use of a time variant generated key as taught by Lennon et al. in order to protect unauthorized access to the content.

7. **Claim 4** is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al.(US 5,054,064 dated 10/01/1991) in view of Choi et al. (US 2002/0194492 dated 12/19/2002).

Walker et al. discloses a video system that includes a central facility (external device) and a terminal. The video system is provided with the video program, which is transmitted, by broadcast, cable, satellite, fiber or any other transmission medium (It is factual information that the content is being sent from a server; col. 2 lines 30 – 32). The terminal includes means for

retrieving video programs and sending the program identification data to the central facility (yourdictionary.com states: download means to transfer (data or programs) from a server or host computer to one's own computer or device. Similarly upload means to transfer (data or programs), usually from a peripheral computer or device to a central, often remote computer. Therefore, here transmitting or receiving content means downloading or uploading content, as content is being transferred over a network). The central facility includes a database for storing and retrieving at least one code encryption code corresponding to the program identification data and means for sending the code encryption key from the central facility to the terminal (abstract). The terminal includes means to store terminal identification data, means to send the central facility the terminal identification data and the program identification data over link (a link is a continuous data channel between a terminal and a central facility such as an ISDN D-channel or by modem a regular phone line (col. 3 lines 46-49)) (col. 2 lines 44-47). The terminal receives the code encryption key from the central facility and decrypts the encrypted digital code (claim 1, lines 14-22). The terminal includes a controller, an encryptor, and a decryptor and recording medium (storage) to store the signal, a memory to store the key and terminal ID (Fig. 1, col. 2 lines 21-45; col. 3 lines 5-15). Terminal includes means to encrypt the terminal identification data according to the terminal specific encryption key, means to send unencrypted terminal identification data and encrypted terminal identification data to the central facility, which in turn includes means to compare unencrypted and encrypted terminal identification data to verify terminal identity (col 3. lines 15-21). The system preferably uses at least one downloadable key, encrypted video program that uses the key for decryption, and data stored a field of the video program. It may be implemented in all digital, analog or mixed

analog/digital environments (col. 4 lines 22-26). DES decryption keys are transmitted from the central facility to the terminal. The DES session key is generated by the central facility at the beginning of the session and remains valid for the duration of the session. The terminal begins the session using a terminal-unique DES key stored in a ROM (col. 5 lines 32-39).

Walker et al. discloses all the limitation of claim 4 except for generating the encryption key based on model information and a serial number of the mobile terminal as an obvious encryption technique as illustrated by Choi et al. which discloses a program that generates a system unique encryption key from the unique hardware information (serial number, model information, etc.) of a personal computer [0076]. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al. to include the use of an encryption key generated based on model information and serial number as taught by Choi et al. in order to limit the access of the content only by a key manager as stated by Choi et al. ([0077] lines 8-11).

8. **Claim 5** is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (US 5,054,064 dated 10/01/1991) and Choi et al. (US 2002/0194492 dated 12/19/2002) as applied to independent claim 4 above, and further in view of Lennon et al. (US 4193131 dated 03/11/1980).

Walker et al. and Choi et al. disclose all the limitations of claim 5 except that the encryption key is generated by the external device considering further time information set in the external device. The general concept of generating encryption keys using time information set is well known in the art as an obvious encryption technique as illustrated by Lennon et al. which discloses a system generated time variant, dynamically created key being transmitted in enciphered form under key encrypting key from a host system to a remote terminal [col. 6 lines

27-31]. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al. and Choi et al. to include the use of a time variant generated key as taught by Lennon et al. in order to protect unauthorized access to the content.

9. **Claim 6** is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (US 5,054,064 dated 10/01/1991), Choi et al. (US 2002/0194492 dated 12/19/2002) and Lennon et al. (US 4193131 dated 03/11/1980) as applied to claim 5 above, and further in view of Yamamoto et al. (US 6307940 dated 10/23/2001).

Walker et al., Choi et al, and Lennon et al. disclose all the limitations of claim 6 except for generating the encryption key if the time information set in the external memory device is identical to time information set in the mobile terminal. The general concept of generating encryption key if the time information matches is well known in the art as illustrated by Yamamoto et al. which discloses a block encryption device for performing encryption using a pseudo-random number generated key, if the value in the buffer match with the value in the counter (col. 23 lines 32-48). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al., Choi et al., Lennon et al. and Yamamoto et al. to include the use of generation of encryption key on the basis of time information comparison as taught by Yamamoto et al. in order to restrict access to any machine therefore generating keys only if the information matches.

10. **Claim 7** is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (US 5,054,064 dated 10/01/1991) and Choi et al. (US 2002/0194492 dated 12/19/2002), as applied to claim 4 above, in view of Iguchi et al. (US 2002/0169960 dated 11/14/2002).

Walker et al. and Choi et al. disclose all the limitations of claim 7 except that the mobile terminal transmits a download request signal for the previously uploaded content to the external memory device in response to an input command. The general concept of an input command to transmit or receive content or signals is well known in the art as illustrated by Iguchi et al. which discloses a host interface for transmitting/receiving an access command between the storage device and an external appliance connected to the storage device, where the input/output interface performs processings such as a key inputting by the user of the mobile terminal and a screen displaying [0041] and the transmission/reception (of the information between the storage device and the mobile terminal is performed by the access command [0062-0063]. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al. and Choi et al. to include the use of an input command as taught by Iguchi et al. in order to better transmit information.

11. **Claims 8 and 9** are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (US 5,054,064 dated 10/01/1991) in view of Kii et al. (US 20020099661 dated 07/25/2002) and Choi et al. (US 2002/0194492 dated 12/19/2002).

Walker et al. discloses a video system that includes a central facility (external device) and a terminal. The video system is provided with the video program, which is transmitted, by broadcast, cable, satellite, fiber or any other transmission medium (It is factual information that the content is being sent from a server; col. 2 lines 30 – 32). The terminal includes means for retrieving video programs and sending the program identification data to the central facility (yourdictionary.com states: download means to transfer (data or programs) from a server or host computer to one's own computer or device. Similarly upload means to transfer (data or

programs), usually from a peripheral computer or device to a central, often remote computer. Therefore, here transmitting or receiving content means downloading or uploading content, as content is being transferred over a network). The central facility includes a database for storing and retrieving at least one code encryption code corresponding to the program identification data and means for sending the code encryption key from the central facility to the terminal (abstract). The terminal includes means to store terminal identification data, means to send the central facility the terminal identification data and the program identification data over link (a link is a continuous data channel between a terminal and a central facility such as an ISDN D-channel or by modem a regular phone line (col. 3 lines 46-49)) (col. 2 lines 44-47). The terminal receives the code encryption key from the central facility and decrypts the encrypted digital code (claim 1, lines 14-22). The terminal includes a controller, an encryptor, and a decryptor and recording medium (storage) to store the signal, a memory to store the key and terminal ID (Fig. 1, col. 2 lines 21-45; col. 3 lines 5-15). Terminal includes means to encrypt the terminal identification data according to the terminal specific encryption key, means to send unencrypted terminal identification data and encrypted terminal identification data to the central facility, which in turn includes means to compare unencrypted and encrypted terminal identification data to verify terminal identity (col 3. lines 15-21) as required by claim 9. The system preferably uses at least one downloadable key, encrypted video program that uses the key for decryption, and data stored a field of the video program. It may be implemented in all digital, analog or mixed analog/digital environments (col. 4 lines 22-26). DES decryption keys are transmitted from the central facility to the terminal. The DES session key is generated by the central facility at the beginning of the session and remains valid for the duration of the

session. The terminal begins the session using a terminal-unique DES key stored in a ROM (col. 5 lines 32-39).

Walker et al. discloses all the limitations of claim 8 and 9 except that the external device generates an encryption key based on the model information and the serial number of the mobile terminal. The general concept of generating an encryption key based on the model information and serial number is well known in the art as illustrated by Choi et al. discloses a program that generates a system unique encryption key from the unique hardware information (serial number, model information, etc.) of a personal computer [0076].

Walker et al. and Choi et al. disclose all the limitations of claim 8 except for transmitting content upload request signal to the external memory. The general concept of sending an upload signal is well known in the art as illustrated by Kii et al.which discloses user terminal device sending a content download request to the service provider [0393] and a management unit receiving a content upload request command from the user terminal device [0470].

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al. to include the use of an encryption key generated based on model information and serial number as taught by Choi et al. in order to limit the access of the content only by a key manager as stated by Choi et al. ([0077] lines 8-11).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al. to include the use of content upload request signal in order to communicate between terminals as an obvious communication technique.

12. **Claim 10** is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (US 5,054,064 dated 10/01/1991), Kii et al. (US 20020099661 dated 07/25/2002) and Choi et al. (US

2002/0194492 dated 12/19/2002) in further view of Hirasawa et al. (US 2003/0061196 dated 03/27/2003).

Walker et al., Kii et al., and Choi et al. disclose all the limitations of claim 10 except for selection of a content index information for downloading from content index information provided from the external memory device. The general concept of downloading information from an external device is well known in the art as illustrated by Hirasawa et al. which discloses the content obtaining unit which searches the content database for the contents corresponding to the index information included in the download instruction, and generates the download contents as the respective copies of the retrieved contents [0120]. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al., Kii et al., and Choi et al. to include the use of a content index information for downloading in order to download specific information stored in the external device.

13. **Claim 11** is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (US 5,054,064 dated 10/01/1991), Kii et al. (US 20020099661 dated 07/25/2002) and Choi et al. (US 2002/0194492 dated 12/19/2002) as applied to independent claim 8 above, and further in view of Lennon et al. (US 4193131 dated 03/11/1980).

Walker et al., Kii et al. and Choi et al. disclose all the limitations of claim 11 except that the encryption key is generated by the external device considering further time information set in the external device. The general concept of generating encryption keys using time information set is well known in the art as an obvious encryption technique as illustrated by Lennon et al. which discloses a system generated time variant, dynamically created key being transmitted in enciphered form under key encrypting key from a host system to a remote terminal [col. 6 lines

27-31]. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al., Kii et al. and Choi et al. to include the use of a time variant generated key as taught by Lennon et al. in order to protect unauthorized access to the content.

14. **Claim 12** is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (US 5,054,064 dated 10/01/1991), Kii et al. (US 20020099661 dated 07/25/2002), Choi et al. (US 2002/0194492 dated 12/19/2002) and Lennon et al. (US 4193131 dated 03/11/1980) as applied to claim 11 above, and further in view of Yamamoto et al. (US 6307940 dated 10/23/2001).

Walker et al., Kii et al., Choi et al, and Lennon et al. disclose all the limitations of claim 12 except for generating the encryption key if the time information set in the external memory device is identical to time information set in the mobile terminal. The general concept of generating encryption key if the time information matches is well known in the art as illustrated by Yamamoto et al. which discloses a block encryption device for performing encryption using a pseudo-random number generated key, if the value in the buffer match with the value in the counter (col. 23 lines 32-48). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Walker et al., Kii et al., Choi et al., Lennon et al. and Yamamoto et al. to include the use of generation of encryption key on the basis of time information comparison in order to restrict access to any machine therefore generating keys only if the information matches.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Supriya Ahuja whose telephone number is 571-270-1588. The examiner can normally be reached on Monday - Thursday 7:30 -5:00; 2nd Friday 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Jules can be reached on 571-272-1808. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Supriya Ahuja

S.A.
February 12, 2007

FRANTZ JULES
SUPERVISORY PATENT EXAMINER